I. Introduction and Overview

The Federal Trade Commission (the "FTC" or "Commission") submits this Report pursuant to Section 9 of the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (the "CAN-SPAM Act"), 15 U.S.C. § 7708 (2003), which requires the Commission to: (1) prepare a report setting forth a plan and timetable for establishing a National Do Not Email Registry; (2) explain any practical, technical, security, privacy, enforceability, or other concerns that the Commission has regarding such a Registry; and (3) explain how such a Registry would be applied with respect to children with email accounts.[1]

Unsolicited commercial email ("UCE" or "spam") poses a serious threat to electronic communication over the Internet for consumers and businesses. Deception and fraud appear to characterize the vast majority of spam.[2] Spam, even if not deceptive, may also lead to significant disruptions and inefficiencies in Internet services as when it spreads viruses that wreak havoc for computer users. Moreover, a serious Internet infrastructure problem flows from the sheer volume of spam that is now being sent. These problems are significant for consumers and businesses and threaten their confidence in the Internet as a medium for communication.

Solving the spam problem begins with recognition that spammers are essentially anonymous. The current email system enables spammers to hide their tracks and thereby evade ISPs' anti-spam filters and law enforcement. A prerequisite for fighting spam is ending this anonymity through a robust authentication standard that ensures that a message actually comes from the domain listed in the message's headers. Without authentication, a Registry will, at best, have no impact on spam and, at worst, result in more spam. Effective authentication would improve CAN-SPAM Act compliance and, coupled with better filtering by ISPs, would greatly reduce the volume of spam.

This Report therefore proposes a plan that recognizes the need for an authentication standard.[3] Section II of this Report describes the

1. Section 9 of the CAN-SPAM Act provides:

   Not later than 6 months after December 16, 2003, the Commission shall transmit to the Senate Committee on Commerce, Science, and Transportation and the House of Representatives Committee on Energy and Commerce a report that –

   (1) sets forth a plan and timetable for establishing a nationwide marketing Do-Not-E-Mail Registry;

   (2) includes an explanation of any practical, technical, security, privacy, enforceability, or other concerns that the Commission has regarding such a Registry; and

   (3) includes an explanation of how the Registry would be applied with respect to children with e-mail accounts.

2. In an April 2003 study of over 1000 pieces of spam, Commission staff found that about two-thirds of the spam analyzed contained likely false claims in the "From:" line, "Subject:" line, or message text. False Claims in Spam, 10. Further analysis revealed that 84.5 percent of the spam analyzed were deceptive on their face or advertised an illegitimate product or service. The Commission has posted the False Claims in Spam report online at http://www.ftc.gov/reports/spam/030429spamreport.pdf.

3. A mechanism for shifting the cost of spam from the recipient to the sender would also contribute to solving the spam problem by addressing another fundamental problem, namely, the low cost of sending spam. The Commission does not presently propose a mechanism for accomplishing such a cost shift because numerous issues exist regarding who should pay for the cost of email, who should be paid, how much should be paid, and the mechanism for collecting and distributing such payments. In addition, cost-shifting would require a more fundamental Internet protocol change whereas authentication standards are at the point where they can be tested and implemented in the near term.

information gathering methods the Commission used to prepare this Report. Section III provides a basic explanation of the email system, including how it enables spam by permitting the sending of unauthenticated messages and how the creation of an authentication system is a first step to help bring the spam epidemic under control. Section IV describes three possible models for a National Do Not Email Registry and explains the practical, technical, security, privacy, enforceability, and other concerns that the Commission has regarding each Registry model. Finally, Section V sets forth a plan and timetable for establishing a Registry.

II. Information Gathering Processes

In preparing this Report on a National Do Not Email Registry, the Commission used a number of information-gathering techniques to obtain information from dozens of individuals and organizations. First, the Commission issued a Request for Information ("RFI") seeking detailed Registry proposals from businesses with the technological skill to design and manage a Registry.[4] The RFI described various formats for a possible Registry and invited responders to use their technical skill and creativity to design alternative formats. The Commission received 13 responses to the RFI, ten of which proposed the creation of a Registry.[5] These ten responses provided the Commission with detailed information that greatly assisted its analyses of the practical, technical, security, privacy, and enforceability issues surrounding a Registry.

Second, between January and March 2004, the Commission interviewed over 80 individuals representing 56 organizations, including consumer groups, email marketers, Internet Service Providers ("ISPs"), law enforcement, private attorneys with spam enforcement experience, and technologists.[6] A court reporter transcribed most of these interviews.[7] These interviews enabled the Commission to draw upon the skills and backgrounds of a wide variety of organizations.

Third, using its compulsory process powers under Section 6(b) of the FTC Act, 15 U.S.C. § 46(b), the Commission required the seven ISPs that collectively control over 50% of the market for consumer email accounts to provide detailed information concerning their experiences with spam.[8] The 6(b) Orders asked for data concerning the volume and types of spam hitting these companies' mail servers and being delivered to their subscribers' inboxes. The 6(b) Orders also required the ISPs to provide detailed information regarding their anti-spam technologies and enforcement efforts.[9]

4. The RFI is attached as Appendix 1.
5. All but one of the RFI responders requested that their responses be treated as confidential. This Report, therefore, does not identify the RFI responders or describe confidential details of their proposals.
6. A complete list of interviewees has been attached to this Report as Appendix 2.
7. Citations to these transcripts identify the organization, representative from the organization, and page number of the transcript. For instance, the citation "Microsoft: Goodman, 16," would refer to a statement made by Microsoft employee Joshua Goodman on page 16 of the transcript. The Commission has posted the transcripts online at http://www.ftc.gov/reports/dneregistry/xcripts/index.pdf.
8. The Commission issued 6(b) Orders to America Online, Comcast, Earthlink, Microsoft, MCI, United Online, and Yahoo!.
9. To ensure that their anti-spam techniques do not become known to spammers, the ISPs have

Fourth, the Commission solicited comments from the general public in a March 11, 2004 Advance Notice of Proposed Rulemaking concerning CAN-SPAM Act rules (the "ANPR").[10] By the close of the comment filing period, the Commission received 7,147 comments regarding the creation of a National Do Not Email Registry.[11]

Finally, to ensure that the Commission's assessment of the technological and security issues posed by a possible Registry were well-grounded, the Commission retained the services of three preeminent computer scientists: Edward W. Felten, Associate Professor of Computer Science at Princeton University; Matthew Bishop, Associate Professor of Computer Science at the University of California ("UC") Davis and Co-director of the UC Davis Computer Security Laboratory; and Aviel Rubin, Professor of Computer Science at Johns Hopkins University and the Technical Director of Johns Hopkins' Information Security Institute.[12] The Commission retained these three experts because of their extensive background in analyzing the security of large computer systems. These experts have conducted independent appraisals of the security and technical issues surrounding a possible National Do Not Email Registry, and their assessments provide unbiased views of the challenges involved in creating a viable National Do Not Email Registry.[13]

III. The Email System and the Resulting Spam Problem

The email system is open, allowing information to travel freely with relative anonymity and ease. This structure facilitates the proliferation of spam by making it possible and cost-efficient for illegitimate marketers to send spam to billions of email accounts worldwide, while allowing them to hide

requested confidential treatment of their 6(b) Order responses. When possible, the Commission has aggregated data from these responses. When the Commission relies on a 6(b) Order response from a particular ISP, this Report does not identify the particular ISP.

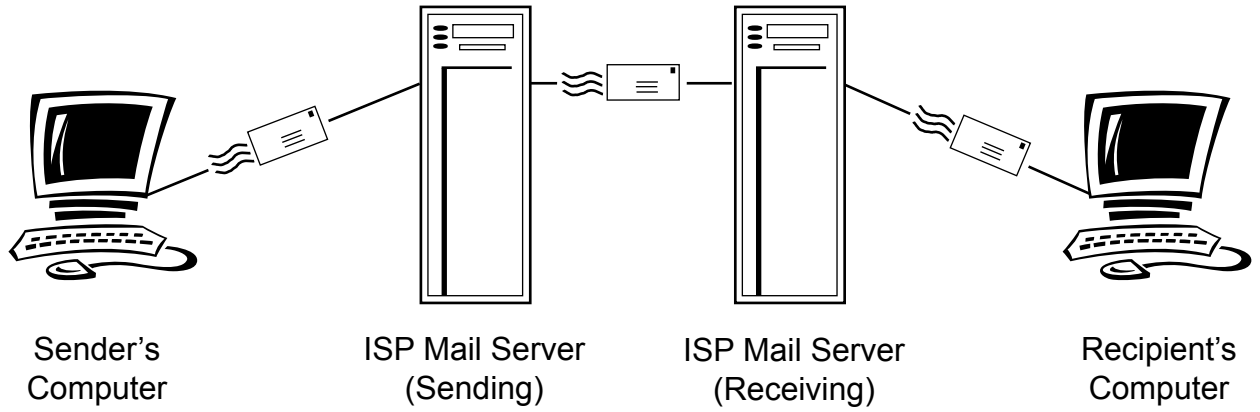
10. Citations to these comments identify the organization or person submitting the comment and the page number of the comment. For instance, the citation "DMA-Comment, 3" refers to page 3 of the comment submitted by the Direct Marketing Association. The Commission has posted the comments online at http://www.ftc.gov/os/comments/canspam/index.htm.

11. Over 6,000 of these comments were form letters from members of the National Association of Realtors arguing that a Registry would impose a significant burden on legitimate businesses while doing little to control abusive spammers. Forty of the total comments were from various industry groups, trade associations, consumer groups, educational institutions, and a government entity, of which at least 34 opposed a Registry based on practical, technical, privacy, and security concerns. The remaining 797 comments, which varied in scope and substance, were from individuals.

12. The Commission has posted reports prepared by these three computer scientists online at http://www.ftc.gov/reports/dneregistry/expertrpts/index.pdf. Citations to these expert reports identify the name of the expert and the page of the report. For instance, the citation "Bishop Report, 2" refers to a statement appearing on page 2 of the report prepared by Matthew Bishop, Ph.D.

13. The Commission's considerable prior experience with the issue of spam, including its enforcement experience and the Spam Forum, a three-day conference held in the Spring of 2003, also guides its analyses of the issues discussed in this Report. The Commission has posted transcripts of the Spam Forum online at http://www.ftc.gov/bcp/workshops/spam. Citations to the transcripts of the Spam Forum identify the speaker's organization and name, the date of the Forum, and the page number on which the statement can be found. For instance, the citation "Aristotle: Shivers - Spam Forum (May 1, 2003), 30" would refer to a statement made by Aristotle employee Carl Shivers that can be found on page 30 of the May 1, 2003 Spam Forum transcript.

Graphic 1



their identities and the origins of their email messages. ISPs have responded to the spam problem by using blocking and filtering software. Currently, ISPs are attempting to combat this fundamental problem with spam – anonymity – by developing authentication technologies that would provide a method for identifying the true origin of an email.

A. How the Email System Works[14]

Email is a complex system that includes the sequential interactions of at least four computers[15] that engage in a five-part dialogue. (*See* Graphic 1). Each step in the email process is recorded within the email's "headers," so that an email's path through each computer can be tracked. Unfortunately, the system that makes email work, "Simple Mail Transfer Protocol" or "SMTP,"[16] does not require the transmission of accurate information. As explained below, the only piece of information that must be accurate is the recipient's address appearing in an SMTP command known as "RCPT TO."

1. The five-part dialogue

Anyone who has ever used email knows what a "user-friendly" medium it is. To send a message, a person only needs to open an email program, type a recipient's address in the "To:" line, perhaps include a subject in the "Subject:" line, type the body of the message, maybe add an attachment, and select "send." A recipient has a similarly easy time. To read a message, a recipient only needs to open an email program, select the message listed in the inbox, and, if an attachment is included with the message, download or read the attachment.

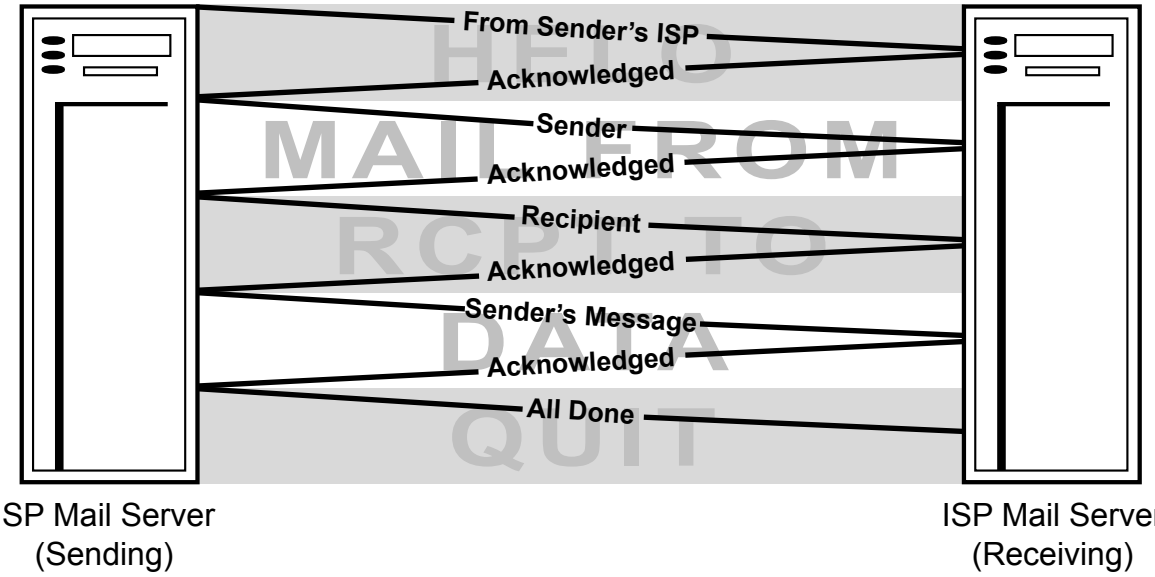
The technical process of how email functions is, of course, much more complex. From the time that a person clicks "send" until the message arrives in a recipient's inbox, many processes occur involving – when reduced to the most basic form – at least four computers:

14. Don Blumenthal, the FTC's Internet Lab Coordinator, provided much of the material for this Section.

15. In reality, if a message is sent within an organization, only three computers may be involved because the sending mail server and the receiving mail server may be the same.

16. SMTP is defined in a "request for comments" posted by the Internet Engineering Task Force ("IETF") and known as RFC 2821. The IETF is an Internet-standards setting body.

Graphic 2



(1) the sender's computer; (2) a mail server owned by an ISP or other entity that provides the sender with an email account; (3) a mail server owned by an ISP or other entity that provides the recipient with an email account; and (4) the recipient's computer.

Clicking the "send" button transmits the email message from the sender's computer to the sender's outbound mail server. This sending server locates and begins a dialogue with the recipient's inbound mail server using SMTP. Under SMTP, the sending and receiving mail servers engage in a five-part dialogue. (*See* Graphic 2).

In the first part, the sending server initiates the exchange with the receiving server using a command known as "HELO," followed by the name of the sending mail server. If translated into English, the sending server would be saying "Hello, I'm <servername>." The receiving server responds with an acknowledgment back to the sending server. It is important to note that the receiving server uses this "HELO" command only to ensure that it is receiving a valid transmission.[17] The receiving server does not verify whether the servername listed after the "HELO" command is the sending server's actual, accurate name. This aspect of SMTP – the fact that the receiving server does not demand authentication that the sending server is what it purports to be – significantly impedes effective anti-spam solutions, including robust enforcement of the CAN-SPAM Act and the effective use of anti-spam filters by ISPs and other domain operators.[18]

After the receiving server has sent an acknowledgment, the sending server begins the second part of the dialogue, using a command called "MAIL FROM." The sending server, in effect, tells the receiving server, "I have mail to deliver from <sender>." The "MAIL FROM"

17. The receiving computer only validates whether the dialogue started properly. The "HELO" command is the first command allowed under the SMTP system. If there is no "HELO" command when using SMTP, then the transmission is invalid.

18. *See infra* Section III.B.1.

is followed by an email address, known as the "envelope from." The "envelope from" is analogous to the return address appearing on an envelope sent through the postal system. As with a return address on an envelope, nothing requires the "envelope from" to be accurate. Moreover, just as the return address on a letter need not match the return address on the envelope containing the letter, the "envelope from" does not have to match the "From:" line that a recipient sees when reading an email message.[19]

In the third part of the dialogue, the sending server, using the "RCPT TO" command, tells the receiving server the email address to which the message should be delivered, and the receiving server sends an acknowledgment back to the sending server. If the message is for more than one recipient, the sending server issues separate "RCPT TOs" for each one. As with the "MAIL FROM," nothing requires that the "RCPT TO" address match the address that appears in the "To:" line of the email. Spammers often exploit this feature to make it appear that their messages are personal. For example, a message's "To:" line may state "Bob," "Account Holder," or any other term designed to trick recipients into believing that they have a relationship with the spammer. In contrast, the email address in the "RCPT TO" command must be valid or the message cannot be delivered.[20]

In the fourth part of the dialogue, after the receiving server has acknowledged the "RCPT TO," the sending server, using the "DATA" command, transmits the actual message. While not required, the first line of the message usually begins with "Subject:," followed by the sender's desired subject. Other headers, such as "Reply-To:,"[21] "cc:," and "bcc:" also may be specified here.[22] The text of the message and any attachments then follow. A blank line with a period signals the end of the "DATA" section. This part of the dialogue concludes when the receiving mail server acknowledges receipt of the email.

In the fifth and final part of the dialogue, the sending server uses the "QUIT" command to terminate the process. The recipient then can view the message through a web interface or email program.

2. Email headers

In theory, the above-described email path is memorialized in "headers" that the recipient can view. Headers are added at three points in the basic four-computer model: (1) message creation; (2) transmission to the sender's server; and (3) transmission to the recipient's

19. Indeed, the Commission staff's April 2003 False Claims in Spam Study reported that 1/3 of the spam analyzed contained false information in the "From:" line. False Claims in Spam, 3.

20. *See infra* Section III.B.1.

21. "Reply-To:" may vary from the address in the "From:" line. This header has legitimate uses; for example, a sender with two addresses may want replies to go to only one address. Spammers, however, can use this header to deflect hostile responses. For instance, the "Reply-To:" address may identify a non-existent email address, in which case opt-out demands will disappear into the ether. Or, the spammer may identify a valid but innocent email address, thereby causing the maligned addressee to receive an avalanche of opt-out requests and complaints. *See infra* Section III.B.1.

22. The headers discussed in this section are only a subset of those available. They are, however the most commonly used and the most important for understanding email transmission and how spammers use the current system to hide their identities.

#	Header	Header's Source
1	Received: from server.sender.com (server.sender.com [123.45.67.90]) by server.recipient.com (8.8.5/8.7.2) with ESMTP id ABC12345 for <pan@recipient.com>; Tue, Mar 30 2004 20:06:22 EST -0500 (EST)	Receiving Mail Server
2	Received: from client.sender.com (client.sender.com [123.45.67.89]) by server.sender.com (8.8.5) id 003A23; Tue, Mar 30 2004 20:06:17 EST -0500 (EST)	Sending Mail Server
3	From: dmb@sender.com (D.M. Bloom)	Sender
4	To: pan@recipient.com	Sender
5	Date: Tue, Mar 30 2004 20:06:15 EST	Sending Mail Server
6	Message-Id: <dmb061346790416-00012487@sender.com>	Sending Mail Server
7	X-Mailer: Eudora v.6.0.3.0	Sender's Computer
8	Subject: How Email Works	Sender

server. Headers contain lines of information that provide details about the message and its transmission. Understanding headers is critical to understanding how email works and how spammers exploit the email system.

When an email is received, the recipient usually views only a few of the header lines, including the "To:" line, the "From:" line, the "Subject:" line, and the "Date:" line. Most email programs, though, enable recipients to view all of the headers for each message. A recipient who chooses to view all headers will see the information appearing in the second column of the table above, showing an illustrative email header, presented in the order in which it appears in the email.[23]

As a message travels from computer to computer, a new header is added to the top of the list of headers. Headers therefore should be read in reverse order. In the example above, the sender creates Line 8, the "Subject:" header. The sender's computer also creates Line 7, "X-Mailer," a header that denotes the sender's email program. The sender's mail server adds Line 6, the "Message-Id," a unique number that stays with the message from beginning to end. (Other "Ids" are created as the message passes through different servers). The "Message-Id" does not always have the email format shown here; it may be just a series of characters without the sender's domain information.[24] The sender's mail server adds Line 5, "Date:." This header shows the date and time the sender's mail server processes the message. Line 4, "To:," shows the intended recipient, and line 3, "From:," shows the sender's email address. The sender creates both Lines 4 and 3. "From:" also may show a name in brackets or parentheses.

Headers that begin with "Received:" are called "routing headers," and each mail server that a message passes through as it travels from sender to recipient adds such a routing header. These headers should be read from bottom to top. In the example above, the first "Received:" header (Line 2) indicates that the sending mail server (server.sender.com) received the message from the sender's computer (client.sender.com), which had the IP number, or Internet address, 123.45.67.89, on March 30, 2004, at 8:06 pm. The "8.8.5" shows

23. In reality, each line of an email header is not numbered, although for convenience of explanation, the table provides ordinal numbers in the first column.

24. The sender's domain information – where on the Internet the sender purports to come from – appears after the @ symbol in line 6.

the version of Sendmail, a mail server program, used on the sender's server. The second "Received:" header (Line 1) shows receipt of the message by the recipient's mail server from the sender's mail server. This header is similar to the previous one except for the format of the "ID" assigned at this step and the fact that it shows the intended recipient. The routing is now complete; the recipient's email program does not add a header when the message is retrieved.

The four-computer model is the simplest depiction of the core processes in sending an email message. Email routing is rarely that simple, however. There are almost always a number of additional intervening stops on the path from sender to recipient. This is because the sender's mail server must find the proper IP address for the recipient's mail server. If the sending server does not have a complete database of email servers and their corresponding IP addresses, it must route the message through intervening servers, or "relays," that narrow the destination down to the proper receiving server. Each server in the relay process adds a "Received from:" line to the headers.[25] When relays are secured properly, the system works well and a message can be traced to its origin.

B. How Spammers Exploit the Email System

Spammers are technologically adept at hiding their identities. Their concealment techniques make it extremely difficult to track them. In addition, spammers continually engage in a game of technological cat-and-mouse with the ISPs that try to block their messages.

1. Spammers exploit SMTP's anonymity

Spammers use many techniques to hide, including: spoofing, open relays, open proxies, and zombie drones. As explained below, each of these techniques makes it difficult, if not impossible, to identify spammers through email headers and significantly impedes law enforcement.[26]

First, spammers use "spoofing" to falsify header information and hide their identities. This technique disguises an email to make it appear to come from an address other than the one from which it actually comes.[27] A spammer can falsify portions of the header or the entire header. A spammer can even spoof the originating IP address.[28] The SMTP system facilitates this practice because it does not require accurate routing information except for the intended recipient of the email.[29] By failing to require accurate sender identification, SMTP allows spammers to send email without accountability, often disguised as personal email.[30] A spammer can send out millions of spoofed messages, but any bounced messages – messages returned

25. As part of the Data dialogue in part 4 of the SMTP dialogue described above, spammers also can add spurious "Received:" headers manually before sending a message.

26. *See infra* Section III.C.

27. Felten Report, 2. Spoofing requires virtually no technical sophistication and can be accomplished by simply changing the preferences in a computer user's email software. AOL: Koschier – Spam Forum (April 30, 2003), 175-82.

28. Bishop Report, 12 n.6.

29. *See supra* Section III.A.1.

30. An attorney representing AOL testified before the Pennsylvania State Senate Communications and Technology Committee that as much as 90 percent of spam messages contain falsified header or routing information (September 23, 2003).

as undeliverable – or complaints stemming from the spoofed emails will only go to the person whose address was spoofed. The spammer never has to deal with them. As a result, an innocent email user's inbox may become flooded with undeliverable messages and angry, reactive email, and the innocent user's Internet service may be shut off due to the volume of complaints.[31]

Second, spammers use open relays to disguise the origin of their email. The difference between an open relay and a "secure" one is critical. A computer must be connected to a mail server to send or receive mail. When someone sends an email message using an email server that is "secure," the mail server's particular software checks to make sure that the sender's computer and email account are authorized to use that server. If this authorization is in order, then the server sends the mail. If the computer and email account are *not* listed as authorized, the server refuses to accept the email message. On the other hand, if a mail server is *not* secure, i.e., some of its settings allow it to stay open, it will forward email even though the senders are not authorized users of that server. An open server is called an open relay because it will accept and transfer email on behalf of any user anywhere.[32]

Spammers who use open relays effectively bypass the email servers to which their computers are connected. Once the spam passes through an open relay, a routing header from that server is added to the email. Thus, the email will appear as if it originated from the relay mail server. This allows spammers to obscure their tracks, making it difficult to trace the path their message takes from sender to recipient.

Third, many spammers use "open proxies." They began doing this after ISPs and other mail server operators realized the negative impact of open relays and made efforts to identify and close them.[33] Again, a word of explanation is in order. Most organizations have multiple computers on their networks, but have a smaller number of proxy servers that are the only machines on the network that directly interact with the Internet.[34] This system provides more efficient web browsing for the users within that organization and secures the organization's network against unauthorized Internet users from outside the organization. If the proxy is not configured properly, it is considered to be "open," and may allow an unauthorized Internet user to connect through it to other hosts (computers that control communications in a network or administer databases) on the Internet. "[P]roxy misconfiguration is common and results in general purpose forwarding that is utilized by hackers and spammers."[35] For example, a spammer can use an open proxy to connect to another mail server and use that mail server to

31. The Commission has charged spoofing as a violation of Section 5 of the FTC Act, 15 U.S.C. § 45. *See e.g., FTC v. GM Funding*, No. SAVC 02-1026 (C.D. Cal. filed Nov. 6, 2002) (one victim of spoofing received 40,000 rejected messages in his inbox); *FTC v. Westby*, No. 032-3030 (N.D. Ill. filed Apr. 15, 2003). Moreover, spoofing violates Sections 4 and 5(a) of the CAN-SPAM Act, 18 U.S.C. § 1037 and 15 U.S.C. § 7704(a).

32. Rubin Report, 13.

33. Nonetheless, "open relays continue to exist in abundance." Rubin Report, 14.

34. A proxy server is so named because, when interacting with the Internet, it serves as a substitute or proxy for other computers on its network.

35. Rubin Report, 14.

send spam. The headers for messages that pass through an open proxy indicate the proxy's IP address in the "Received:from" line, and not the true originating IP address. In this way, open proxies provide another means for spammers to hide their tracks. MessageLabs, an email security company, believes that spammers sent more than two-thirds of all their email in 2003 through open proxies.[36]

Fourth, the most recent escalation in this cat-and-mouse game involves the exploitation of millions of home computers, using malicious viruses, worms, or "Trojans."[37] These infections, often sent via spam, turn any computer into an open or compromised proxy called a "zombie drone."[38] Once a computer is infected with one of these programs, a spammer can remotely hijack and send spam from it. Spammers target home computers with high speed Internet connections, such as DSL or cable modem lines, that are poorly secured. Spam sent via zombie drones will appear to originate (and actually will originate) from these infected computers.[39] This practice is all the more pernicious because users often do not know that their home computers are infected. The outgoing spam does not show up in their outbox. Once an ISP realizes spam is coming from one of its customer's machines, the ISP must shut off the customer's Internet service even though the customer had no knowledge that the spammer was using his or her machine.[40]

Although it is difficult to estimate the prevalence of zombie drones, Microsoft's Anti-Spam Manager has indicated that zombie drones presently account for somewhere between 15 and 60 percent of spam, and opined that the percentage is rising.[41] One major ISP reported a 41% increase in customer complaints regarding spam coming from other ISPs between October 2003 and February 2004.[42] This ISP believes that the shift is due to the increased use of zombie drones to transmit email messages from those other ISPs.[43] Another ISP reported that during 2003 it discovered over 600,000 open proxies or zombie drones.[44] Most recently, ISPs have observed compromised proxies shifting overseas, which means that the spam looks like it is coming from overseas, yet the virus author and spammer using the drones may be located in the United States.[45] If the past is an indication

36. MessageLabs states its conclusion, but does not explain how the company reached it. MessageLabs, "Spam and Viruses Hit All Time Highs in 2003," December 8, 2003 at http://www.messagelabs.com/news/pressreleases/detail/default.asp?contentItemId=613&region=. A background paper prepared by the Organization for Economic Cooperation and Development ("OECD") in January 2004, similarly states that 50 percent of spam flows through open relays and proxies, but does not explain the basis for this assertion. http://www.olis.oecd.org/olis/2003doc.nsf/43bb6130e5e86e5fc12569fa005d004c/edfc2255d6a8a51ac1256e240030f5b6/$FILE/JT00157096.PDF. The OECD's paper does not indicate the time frame for this statistic.
37. Rubin Report, 14-15.
38. Felten Report, 2.
39. Rubin Report, 14.
40. CNN, "Your Computer Could be a 'Spam Zombie,'" February 18, 2004, at http://www.cnn.com/2004/TECH/ptech/02/17/spam.zombies.ap/.
41. March 10, 2004 briefing of FTC staff by Microsoft Anti-Spam Manager.
42. Confidential 6(b) Order Response.
43. *Id*.
44. Confidential 6(b) Order Response.
45. One ISP reports that in January and February of 2004, 56% of all spam that made it to its subscribers' inboxes was routed through a server or proxy located outside the United States. Confidential 6(b) Order Response.

of the future, within the next several months spammers will have found an as-yet unknown new technique for masking their identities.

2. ISPs' response to spammers' email exploitation

The ISP industry's standard practice is to prohibit unsolicited bulk email.[46] ISPs and email filtering companies attempt to enforce this rule mainly through the use of blocking and filtering software.[47] ISPs initially block email based on volume ("volume filtering") and not based on content because their filters cannot make a distinction between commercial and non-commercial email. Many ISPs first attempt to block email at the point of the attempted connection to the ISPs' networks (the first part of the five-part SMTP dialogue).[48] For example, an ISP may initially block a message based on an IP address it has determined is used by spammers as an open relay or open proxy, or because an IP address or domain is associated with sending high volumes of spam. Anti-spam organizations compile "blacklists" of reported open relays and proxies that ISPs and other operators of mail servers can use to support their filtering efforts.[49]

Although the first line of defense against spam is volume filtering, most ISPs add an additional layer by filtering based upon their own customers' complaints. ISPs use complaint data in a variety of ways, including Bayesian filtering – filtering based upon the concept that some words occur more frequently in known spam. By analyzing email that customers report as spam, ISPs generate a mathematical "spam-indicative probability" for each word.[50] Many email filtering companies combine this type of filtering with filtering based upon different components of the message headers.

ISPs and email filtering companies are concerned about potentially blocking legitimate messages. These "false positives" can be a serious side effect of combating spam. According to Assurance Systems, a spam solutions provider, ISPs block or filter 17% of permission-based email.[51] To reduce false

46. United Online ("UOL"): Popek, 30-31; Junkbusters: Catlett, 15; *See also* the acceptable use policies of MCI (http://global.mci.com/legal/usepolicy; http://privacy.msn.com/anti-spam), Earthlink (http://www.earthlink.net/about/policies/use; http://docs.yahoo.com/info/guidelines/spam.html), Comcast (http://www.comcast.net/terms/abuse.jsp), AOL (http://postmaster.aol.com/guidelines/bulk_email.html), Microsoft (http://privacy.msn.com/anti-spam), and UOL (http://www.netzero.net/legal/terms.html, http://www.juno.com/legal/accept-use.html, and http://www.mybluelight.com/legal/terms-bluelight.html).
47. Email blocking occurs at the point of attempted connection to the ISP's network. Email filtering occurs once an email enters the ISP's network, but before it reaches a recipient's inbox.
48. *See supra* Section III.A.1.
49. SpamCop: Haight – Spam Forum (May 1, 2003), 118.
50. Mertz, David. "Spam Filtering Techniques: Comparing a Half-Dozen Approaches to Eliminating Unwanted Email," Gnosis Software, Inc., August 2002 at http://www.gnosis.cx/publish/programming/filtering-spam.html.
51. http://www.returnpath.biz/pdf/Blocking_Filtering_Report.pdf. Assurance Systems determined the percentage of permission-based messages that were incorrectly filtered by ISPs by tracking the delivery, blocking, and filtering rates of over nine thousand email campaigns. High false positive rates undermine consumer confidence in the email system. In an October 2003 study of 483 randomly selected consumers with home Internet access, RoperASW found that 40 percent of consumers who subscribe to or receive email from their credit card issuer expressed concern about not receiving email from the issuer due to their ISPs' anti-spam filters. *Email and Spam: Attitudes and Behaviors Among Financial Services Consumers*, Study commissioned and submitted to the Commission by Bigfoot Interactive.

positive rates, ISPs compile "white lists" of marketers who agree to adhere to an ISP's policies and procedures regarding bulk email. Once a marketer is on an ISP's white list, the ISP does not filter that marketer's messages. A certain number of complaints regarding a particular marketer who is on the ISP's white list, however, will trigger removal of that marketer from the white list.[52] The threat of false positives is a significant barrier to more effective filtering by ISPs.

C. Email's Lack of Authentication Enables Spammers to Exploit the Email System

Obfuscatory techniques such as spoofing, open relays, open proxies, and zombie drones make it more difficult for ISPs to locate spammers. When ISPs and domain holders implement technologies designed to stop one exploitative technique, spammers quickly adapt, finding new methods to avoid detection. If the cloak of anonymity were removed, however, spammers could not operate with impunity.[53] ISPs and domain holders could filter spam more effectively, and the government and ISPs could more effectively identify and prosecute spammers who violate the CAN-SPAM Act or other statutes.

The marketplace is already moving toward creating systems for authenticating a message's originating second-level domain,[54] with major ISPs backing various approaches.[55] AOL champions the adoption of SPF ("sender policy framework"),[56] an authentication standard developed by Meng Weng Wong ("Wong") that verifies the "envelope from"[57] of an email message. Microsoft has proposed "Caller ID for Email,"[58] a protocol that would verify the "From:" line that appears in an email message.[59] Recently, Microsoft and Wong announced plans to merge SPF and Caller ID for Email into one technical specification.[60] Yahoo! has advocated the implementation of "Domain Keys," a standard that would involve the use of public/private key cryptography.[61] The IETF has also established a working group to develop an authentication standard.[62] The IETF working group intends to propose an authentication standard during the Summer of 2004.[63]

---

52. Briefing of FTC staff by an ISP concerning its Confidential 6(b) Order responses.
53. Comcast: Lutner, 42; Edelman, 28; Savicom: Bernard, 23; UOL: Skopp, 61.
54. A second-level domain is the name in an email address that appears between the "@" symbol and the dot. For instance, "ftc" is the second-level domain in the address "abc@ftc.gov."
55. U.S. Internet Service Provider Association ("USISPA")-Comment, 2 (stating that "several of its members and other technology vendors are in the process of developing solutions to spam based on identifying the origin or identity of email senders"). Digital Impact: Brondmo, 17-18; ESPC: Hughes, 11; Internet Commerce Coalition ("ICC"): Halpert, 25; NetCreations: Mayor, 24; Roving Software: Olson, 20-21.
56. http://www.ietf.org/internet-drafts/draft-mengwong-spf-01.txt.
57. *See supra* Section III.A.1.
58. http://download.microsoft.com/download/2/e/2/2e2850b8-2747-4394-a5a9-d06b5b9b1a4c/callerid_email.pdf.
59. March 10, 2004 briefing of FTC staff by Microsoft Anti-Spam Manager.
60. http://www.microsoft.com/presspass/press/2004/may04/05-25SPFCallerIDPR.asp.
61. http://antispam.yahoo.com/domainkeys.
62. http://www.nwfusion.com/news/2004/0412marid.html.
63. *Id.*

None of these standards has been widely tested, and each is still in development. Estimates differ on how soon the market will test and widely deploy the competing authentication standards. Some believe that all email will be authenticated within a year.[64] Others are less sanguine. According to a technologist with Comcast, "[i]t might be even two years or more before any one solution is solid enough that it can be deployed even in smaller systems where it's not going to crush them."[65] Small ISPs are especially concerned that the multiple authentication standards will prove too costly to implement.[66]

It should be noted that these private market proposals do not authenticate the identity of the person sending an email. In other words, if a message claimed to be from abc@ftc.gov, the private market proposals would authenticate that the message came from the domain "ftc.gov," but would not authenticate that the message came from the particular email address "abc" at this domain. Nonetheless, domain-level authentication would confound spammers' ability to engage in spoofing and to send messages via open relays and open proxies, enable ISPs to deploy more effective filters, and provide law enforcement with an improved ability to track down and prosecute spammers.

64. Digital Impact: Brondmo, 24 (12 months); Roving Software: Olson, 23 (6 to 9 months).

65. Comcast: Lutner, 46.

66. Aritstotle: Bowles, 75.

IV. Possible Models for a National Do Not Email Registry and the Commission's Concerns

In February 2004, the Commission issued an RFI to obtain information from businesses with the technical sophistication to design and manage a National Do Not Email Registry. The RFI described possible models for a National Do Not Email Registry, including the creation of a registry of individual email addresses, a registry of domains, and a registry combined with a certified third-party email forwarding service.[67] The RFI also invited responders to think "outside the box" and stated that "[t]he model registry you propose may consist of . . . an entirely different form of registry."[68]

The Commission received 13 responses. Two provided little useful information, merely advertising their software. One response proposed a dramatic reshaping of the email system that would divide email into classes of

67. The RFI stated that responders should assume that a registry of individual email addresses would include 300 million initial registrations and grow to include as many as 450 million email addresses. In estimating the likely number of registrations, the Commission assumed that the typical Internet user would register between two and three email accounts and that a registry of domains would include 30 million domains. Approximately 150 million American consumers use the Internet. http://www.clickz.com/stats/markets/finance/article.php/5961_3091091. The Commission based its estimate of the number of domains likely to be registered in a domain wide registry on the number of domain names registered in the .com and .org registries. Whois Source, "Detailed Domain Counts and Internet Statistics," April 2004 at http://www.whois.sc/internet-statistics/. Also, following the Do Not Call Model, the RFI posited that a National Do Not Email Registry would include mechanisms to permit consumers to submit complaints (along with offending emails) and to preserve these complaints for future law enforcement purposes.

68. RFI, 2.

users.[69] The remaining ten responses proposed three possible models for a National Do Not Email Registry – a registry of individual email addresses, a registry of domains, and a registry combined with a third-party forwarding service.[70] These ten responses included submissions from some of the largest and most technically-sophisticated Internet, computer, database management, and communications companies in the United States.

Subsection A describes the three proposed Registry models. Subsection B discusses the security and privacy concerns raised by these three models. Subsection C explains the obstacles to enforcing a Registry. Subsection D considers other practical and technical issues raised by a Registry. Subsection E explains why a Registry would fail to reduce the volume of spam hitting consumers' inboxes. Finally, subsection F describes the threat to children with email accounts posed by a National Do Not Email Registry.

A. Proposed Registry Models

1. Registry of individual email addresses

Some of the RFI responses proposed a Registry closely modeled on the National Do Not Call Registry. Such a Registry would consist of a centralized database containing the email addresses of consumers who do not want to receive unsolicited commercial email. These consumers would enter their email addresses on the Registry using a web-based form. Confirmation emails would be sent to the consumers' email addresses. To activate the registration, consumers would return to the Registry's web site and enter a code that appeared in the confirmation email.

Unsolicited commercial email marketers' distribution lists would be scrubbed against the Registry and the addresses on the Registry would be purged from the distribution lists in one of two ways. In a "distributed model," the marketers would receive a copy of the Registry from the Commission, compare their distribution lists to the Registry, and purge from their lists all addresses on the Registry. (This is similar to the process telemarketers use for the National Do Not Call Registry). Alternatively, in a "central-scrubbing model," marketers would submit their distribution lists to the Commission (or the Commission's contractor), which would compare the distribution lists to the Registry and return to each marketer a list with the email addresses appearing on the Registry deleted.

2. Registry of domains

Some RFI responders proposed permitting ISPs and other domain holders to register their objection to receiving spam addressed to

69. The proposed plan would require the FTC to create two classifications of email recipients. Commercial emailers would be prohibited from sending email to the first class of recipients and would be permitted to send email to the second class of recipients only if they had an established business relationship with the recipients. Under the proposal, ISPs would be required to block all commercial email to the first classification of email recipients – those who may not be solicited via commercial email. Such a dramatic reshaping of the email system does not seem practicable at the present time.

70. One of these ten responses proposed a Registry of individual email addresses combined with a mechanism for shifting the cost of email to the sender.

any email addresses located at their domains. According to this model, an official at a domain could inform the Commission that the domain did not want spam sent to any email address located at the domain. For instance, if the domain "ftc.gov" were listed on the Registry, a law-abiding bulk emailer would delete from its mailing list all addresses located "@ftc.gov."[71] Because domain names are already public information, a list of registered domains could be maintained on a public web site. Spam marketers would then be required to scrub their own lists, deleting addresses appearing at domains listed on the Registry.

Some entities have advocated a Domain Wide Registry with the added feature of enabling individual consumers to override their ISP's decision to participate or refrain from participating in a Domain Wide Registry.[72] In other words, with this feature, if a consumer's ISP decided to register its domain as a "no spam" domain, the consumer could still register an email address within this domain that welcomed UCE.

3. Registry of individual email addresses with a third-party forwarding service

Some RFI responders proposed a third-party forwarding service approach, consisting of the creation of a Registry of individual email addresses and a requirement that marketers who use UCE submit their distribution lists and the email messages they wished to distribute to an FTC-approved forwarding service. This service would then scrub the lists against the Registry and forward only those messages that were addressed to recipients whose addresses did not appear on the Registry. Use of the forwarding service could be required of senders of UCE, senders of all commercial messages (whether solicited or not), or even senders of all types of messages (whether "commercial" or not). The marketer would never receive access to the Registry database, nor would it receive its own distribution list purged of email addresses on the Registry.

B. Security/Privacy Concerns

A National Do Not Email Registry containing individual email addresses (or a Domain Wide Registry that permits individuals to override the registration decision of their ISP),[73] would suffer from a significant security weakness that would enable spammers to treat the Registry as the

71. Some entities we spoke with during the preparation of this Report proposed that instead of having a Registry, domain holders could indicate their anti-spam policies by including a notation in the information provided on Domain Name Servers. Anti-Spam Research Group ("ASRG"): Levine, 23; Junkbusters: Catlett, 27-28, 35-36.

72. National Consumers League ("NCL"): Grant, 16-17; Savicom: Bernard, 17; Wilson, Sun, Fee, Goodrich & Risotti ("WSFGR"): Kramer, 14-15; Word to the Wise: Atkins, 39.

73. This critique does not apply to a Domain Wide Registry that prohibits consumers from indicating their individual preferences. Such a model would not be prey to the security and privacy risks described in this portion of the text, because no actual email addresses would be listed on the Registry. Such a Registry, however, would raise serious enforcement and practical concerns. *See infra* Section IV.C and Section IV.D. Similarly, a third-party forwarding service model would significantly reduce the security risks described in this Section because spammers would not be able to use the scrubbing process to validate email addresses. A third-party forwarding service model, however, would be difficult to enforce and would likely result in significant disruption to the email system. *See infra* Section IV.C and Section IV.D.

National **Do** Spam Registry,[74] causing more spam,[75] including more of the most offensive spam, such as pornographic messages, to clog consumers' inboxes and degrade their privacy.[76]

This security weakness – the risk that spammers will use the Registry to determine valid email addresses – exists regardless of whether the Registry is distributed to marketers or centrally-scrubbed by the Commission. The risk that spammers would misuse a Registry is so high that Consumers Union has stated that if the Commission were to adopt an individual email address Registry and distribute the Registry to marketers, it "would emphatically tell all 42 million subscribers [of Consumer Reports] not to sign up for it."[77]

74. Association of National Advertisers-Comment, 2; Innovyx-Comment, 3; USISPA-Comment, 3.

75. American Business Media-Comment, 5; American Council of Life Insurers-Comment, 3; ASRG: Levine, 26-29; Edelman, 8; Greater Washington Community Ass'n of Realtors-Comment, 1; Promotion Marketing Ass'n, Inc.-Comment, 3; UOL: Skopp, 27.

76. "Phishers" pose another security concern for a National Do Not Email Registry. Rubin Report, 13; Comcast: Lutner, 41. "Phishers" are Internet outlaws who collect personal information from consumers by masquerading as companies with whom the consumers have a business relationship. *See, e.g. FTC v. Hill*, No. H 03-5537 (S.D. Tex. 2003). Most phishing schemes have involved spam claiming to be from the billing departments of ISPs and online financial institutions. Government web sites have not been immune to phishing attacks, however. One phisher attempted to trick consumers into providing personal information by claiming to be the web site "regulations.gov." http://www.ftc.gov/bcp/conline/pubs/alerts/phishregsalrt.htm. More recently, in April 2004, a phisher attempted to obtain personal information from consumers by purporting to be the web site www.fdic.gov. http://www.fdic.gov/news/news/press/2004/pr3804.html. A phishing attack against a National Do Not Email Registry could take the form of spam asking recipients to verify their registration status.

77. Consumers Union ("CU"): DeGraff, 29.

Several RFI responders have proposed computer security techniques that they claim would eliminate or alleviate these risks. The Commission has carefully examined these techniques to determine whether these techniques can effectively control these risks, and has concluded that none of them would be effective.

1. The high value of email addresses would likely make a Registry the National *Do* Spam Registry

Unlike the National Do Not Call Registry with which it has been compared, a National Do Not Email Registry would pose substantial security risks because a list of valid email addresses is extremely valuable – far more valuable than a list of working telephone numbers. Telemarketers can easily find working numbers. Unless specifically requested by a subscriber, telephone companies publish telephone numbers in public directories. Moreover, telemarketers can call active unlisted numbers using sequential dialing – an automated method of calling possible telephone numbers in numerical sequence.

Spammers, on the other hand, cannot identify valid email addresses easily. No master list or directory of email addresses exists.[78] As the legal director of the Electronic Frontier Foundation noted:

> I think there's a fundamental difference between telephone numbers and email addresses that plays into this, which is that while telephone numbers really are not "born" private, they are to a certain extent either public or even if you have an unlisted number, pretty easily

78. Felten Report, 2; ASRG: Levine, 15; National Retail Federation ("NRF"): Treanor, 7.

known. Email addresses are "born" private. There is no international or national registry of email addresses that exist[s].[79]

Furthermore, spammers cannot use the equivalent of sequential dialing to reach consumers' inboxes. Although one technique used by spammers approximates sequential dialing, it is far less effective. Spammers can launch a "dictionary attack," which generates email distribution lists by creating a list of alphanumeric character strings that are inserted in front of the "@" sign and then sending a high volume of emails with these character strings to a mail server.[80] The mail server delivers the email to those recipients who accept mail through that server and generally bounces back messages to those recipients who do not. The spammer can use software to track which addresses are valid and which are not, and use that information to create a list of the resulting valid email addresses for future spamming.[81]

The effectiveness of dictionary attacks pales in comparison to that of sequential dialing because of the almost limitless number of possible email addresses. Telephone numbers involve finite combinations of ten digits,[82] but email addresses can contain any number of alphanumeric characters. When a spammer engages in a dictionary attack, it sends a message to a high percentage of undeliverable addresses. The high undeliverable rate triggers the ISPs' filters and results in the ISPs' refusal to deliver the messages.[83] Consequently, spammers prize valid addresses.

Creation of a National Do Not Email Registry database would amount to the compilation of an extensive directory of active email addresses that currently does not exist.[84] According to the Association of National Advertisers, the "Registry would truly be the 'Fort Knox' list of email addresses for a criminal spammer."[85] Further, there seems to be a consensus that while a list of unconfirmed email addresses is valuable to spammers, a list of *live* email addresses would be a gold mine.[86] As the technology stands today, it is impossible to know whether there is a real person behind an email address unless it is tested to verify that it is a valid address.[87] A National Do Not Email Registry database would remove that technological hurdle, one of the

79. Electronic Frontier Foundation ("EFF"): Cohn, 10.

80. For instance, the spammer could send a message to the FTC's mail server addressed to "aaa@ftc.gov," "aab@ftc.gov," "aac@ftc.gov," etc.

81. Postini: McLean - Spam Forum (April 30, 2003), 109-10.

82. A telephone company assigns a subscriber a unique telephone number containing ten digits – a three digit area code, a three digit local exchange, and a four digit number. A sequential dialing program can be programmed to dial only those numbers with valid area codes and local exchanges.

83. Confidential 6(b) Order response.

84. Such a Registry would be a unique source of valid email addresses. ASRG: Levine, 15; Comcast: Lutner, 8; Junkbusters: Catlett, 6; NRF: Treanor, 7.

85. Association of National Advertisers-Comment, 2. According to many the Commission consulted, a list of merely active email addresses is far more elusive and much more valuable than a list of phone numbers. *See* Aristotle: Bowles, 14; ASRG: Levine, 15; Comcast: Lutner, 8; EFF: Cohn, 12; Newsletter & Electronic Publishers Association ("NEPA")-Comment, 2; NortelNetworks: Lewis, 16; Verizon-Comment, 3; Washington Office of Attorney General ("WAOAG"): Selis, 26.

86. Aristotle: Bowles, 15; Comcast: Lutner, 8; EFF: Cohn, 12; NEPA-Comment, 2; NortelNetworks: Lewis, 16; Verizon-Comment, 3; WAOAG: Selis, 26.

87. EFF: Cohn, 12.

only remaining barriers that can slow spammers down.[88] As a Virginia Assistant Attorney General stated:

> [That is] a goldmine that you actually now have confirmed email addresses. There are spammers that spam just to find legitimate email addresses. And you go to a list there that is already guaranteed.[89]

Knowing that they will be reaching millions of people, spammers very likely would pay a premium for a list of active email addresses.[90] Because a Registry likely would be so valuable to spammers,[91] many sources we spoke with expressed serious concern. They are convinced that spammers would stop at nothing to obtain this list and misuse it to the detriment of consumers.[92] The Commission agrees with their assessment.[93]

2. Existing computer security techniques are inadequate

RFI responders proposed three computer security techniques that they claim would significantly reduce the security and privacy risks associated with a Registry of individual email addresses: (1) the centralized scrubbing of marketers' distribution lists; (2) the conversion of addresses to one-way hashes; and (3) the seeding of the Registry with "canary" email addresses. As explained below, while each of these techniques can reduce certain types

88. MCI: Mansourkia, 9.

89. Virginia Office of Attorney General ("VAOAG"): McGuire, 30.

90. CipherTrust: Judge, 29-30; Comcast: Lutner, 8; NortelNetworks: Lewis, 29. It is difficult to predict how much a valid address on the Registry could command in the market. One computer security expert retained by the Commission estimates that a list containing hundreds of millions of addresses would be worth millions of dollars. Rubin Report, 5. The Commission finds this estimate plausible. Unverified addresses sold on the Internet cost fractions of a cent. According to a report at www.internetnews bureau.com, email marketers can rent verified email addresses (for one time use) at a cost of 10 to 40 cents each. http://www.internetnewsbureau.com/ medianet/fourFour.html. A technologist interviewed by the Commission reports that verified email addresses sell for as much as 50 cents each. CipherTrust: Judge, 29. Even if valid addresses on the Registry sold for one cent each, a Registry of 300 million addresses would fetch $3 million.

91. Email marketers can charge their clients using a variety of metrics. For instance, a marketer could charge based on the number of messages sent or even the number of messages opened. As one email marketer who spoke at the Spam Forum explained, by including an html pixel in each message (also known as a "web beacon"), the marketer can tell when a message has been opened. Betterly - Spam Forum (May 1, 2003), 18. For spammers who charge clients based on the number of delivered messages, a list of valid email addresses would be especially valuable. Moreover, according to www.wired.com, a significant number of spammers make money by trafficking in email addresses. For these spammers, a list of valid email addresses would be valuable, as well. http://www.wired.com/news/ebiz/ 0,1272,57613,00.html.

92. Direct Marketing Association ("DMA")-Comment, 9; ESPC-Comment, 7; Junkbusters: Catlett, 6; MBNA: Collingwood, 44-45; NortelNetworks: Lewis, 16; USISPA-Comment, 3; Verizon-Comment, 3; VOAG: McGuire, 29; *but see* NCL-Comment, 3 (NCL does not believe that the information will be used for illegal marketing or malicious purposes because there would likely be substantial penalties for misuse and spammers would refrain from targeting registered addresses because these would be the least likely consumers to be receptive to spam). The Telemarketing Sales Rule includes certain structures and sanctions to prevent misuse of the Registry. See 16 C.F.R. §§ 310.4(b)(2), 310.4(b)(3)(iv), and 310.8. The success of these measures cannot easily be replicated in the email context, however, because the anonymity of email allows spammers to remain hidden and unaccountable for their actions. *See infra* Section IV.C.

93. According to a widely-held view, "[t]here is little reason for a spammer to limit the number of messages sent, or be selective about the chosen recipients, since the marginal cost of every